Please type a plus sign (+) inside this box → [+]

06-29-00

A

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No.	042390.P7709
First Inventor or Application Identifier	Carl M. Ellison
Title	A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY
Express Mail Label No.	EL466332415US

JC571 U.S. PTO 09/605605 06/28/00

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages* 12]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 4]

4. Oath or Declaration [*Total Pages* 4]
a. ☒ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☐ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. ☐ Other: .....

**NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

16. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION or DIVISIONAL APPS only The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* (Insert Customer No. or Attach bar code label here) *or* ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country	U.S.A.	*Telephone*	(714) 557-3800	*Fax*	(714) 557-3347

Name (Print/Type)	William W. Schaal, Reg. No. 39,018		
Signature		*Date*	06/28/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

Our Ref. No. 042390.P7709
Express Mail No.: EL466332415US

UNITED STATES PATENT APPLICATION

FOR

A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY

INVENTORS:

Carl M. Ellison
James A. Sutton

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
(714) 557-3800

A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY

Field

This invention relates to the field of data security. In particular, the invention relates to a platform and method that protects an identity of the platform through creation and use of pseudonyms.

Background

Advances in technology have opened up many opportunities for applications that go beyond the traditional ways of doing business. Electronic commerce (e-commerce) and business-to-business (B2B) transactions are now becoming popular, reaching the global markets at a fast rate. Unfortunately, while electronic platforms like computers provide users with convenient and efficient methods of doing business, communicating and transacting, they are also vulnerable for unscrupulous attacks. This vulnerability has substantially hindered the willingness of content providers from providing their content in a downloaded, digital format.

Currently, various mechanisms have been proposed to verify the identity of a platform. This is especially useful to determine if the platform features a "trusted" device; namely, the device is configured to prevent digital content from being copied in a non-encrypted format without authorization. One verification scheme involves the use of a unique serial number assigned to a platform for identification of that platform. Another verification scheme, performed either independently from or cooperatively with the previously described verification scheme, involves the use of a permanent key pair. The permanent key pair includes (i) a unique public key that identifies the platform and (ii) a private key that is permanently stored in memory of the trusted device. The private key is confidential and is not provided outside the trusted device. However, these verification schemes pose a number of disadvantages.

For example, each of these verification schemes is still subject to data aggregation attacks. "Data aggregation" involves the collection and analysis of data transmitted from a platform over a period of time. Thus, the use of platform serial numbers and permanent keys for identification purposes has recently lead to consumer privacy concerns. Also, for both verification mechanisms, a user cannot

easily and reliably control access to and use of the platform identity on a per-use basis.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a block diagram of an illustrative embodiment of a system utilizing the present invention.

Figure 2 is a block diagram of an illustrative embodiment of the trusted logic employed within the first platform of Figure 1.

Figure 3 is a flowchart of an illustrative embodiment describing allocation and use of a pseudonym produced within the first platform of Figure 1.

Figures 4 and 5 are flowcharts of an illustrative embodiment of the production and certification of pseudonyms.

DETAILED DESCRIPTION

The present invention relates to a platform and method for protecting the identity of the platform through the creation and use of pseudonyms. Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Well-known circuits and cryptographic techniques are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, terminology is used to discuss certain features of the present invention. For example, a "platform" includes hardware and/or software that process information. Examples of a platform include, but are not limited or restricted to any of the following: a computer (e.g., desktop, a laptop, a hand-held, a server, a workstation, etc.); data transmission equipment (e.g., a router, switch, facsimile machine, etc.), wireless equipment (e.g., cellular base station, telephone handset, etc.); or television set-top box. "Software" includes code that, when executed, performs a certain function. "Information" is defined as one or more bits of data, address, and/or control.

With respect to cryptographic functionality, a "cryptographic operation" is an operation performed for additional security on information. These operations may include encryption, decryption, hash computations, and the like. In certain cases, the cryptographic operation requires the use of a key, which is a series of

bits. For asymmetric key cryptography, a device is associated with unique, permanent key pair that includes a public key and a private key.

In addition, asymmetric key cryptography normally utilizes a root certificate. A "root certificate" is a public key at the origination of a digital certificate chain and provides a starting point for all subsequent digital certificates. In general, a "digital certificate" includes information used to authenticate a sender of information. For example, in accordance with CCITT Recommendation X.509: The Directory - Authentication Framework (1988), a digital certificate may include information (e.g., a key) concerning a person or entity being certified, namely encrypted using the private key of a certification authority. Examples of a "certification authority" include an original equipment manufacturer (OEM), a software vendor, a trade association, a governmental entity, a bank or any other trusted business or person. A "digital certificate chain" includes an ordered sequence of two or more digital certificates arranged for authorization purposes as described below, where each successive certificate represents the issuer of the preceding certificate.

A "digital signature" includes digital information signed with a private key of its signatory to ensure that the digital information has not been illicitly modified after being digitally signed. This digital information may be provided in its entirety or as a hash value produced by a one-way hash operation.

A "hash operation" is a one-way conversion of information to a fixed-length representation referred to as a "hash value". Often, the hash value is substantially less in size than the original information. It is contemplated that, in some cases, a 1:1 conversion of the original information may be performed. The term "one-way" indicates that there does not readily exist an inverse function to recover any discernible portion of the original information from the fixed-length hash value. Examples of a hash function include MD5 provided by RSA Data Security of Redwood City, California, or Secure Hash Algorithm (SHA-1) as specified a 1995 publication Secure Hash Standard FIPS 180-1 entitled "Federal Information Processing Standards Publication" (April 17, 1995).

Referring to Figure 1, a block diagram of an illustrative embodiment of a system 100 utilizing the present invention is shown. The system 100 comprises a first platform 110 and a second platform 120. First platform 110 is in communication with second platform 120 via a link 130. A "link" is broadly defined as one or more information-carrying mediums (e.g., electrical wire, optical fiber, cable, bus, or wireless signaling technology). When requested by the

user, first platform 110 generates and transmits a pseudonym public key 140 (described below) to second platform 120. In response, second platform 120 is responsible for certifying, when applicable, that pseudonym public key 140 was generated by a trusted device 150 within first platform 110.

Referring now to Figure 2, in one embodiment, trusted device 150 comprises hardware and/or protected software. Software is deemed "protected" when access control schemes are employed to prevent unauthorized access to any routine or subroutine of the software. More specifically, device 150 is one or more integrated circuits that prevents tampering or snooping from other logic. The integrated circuit(s) may be placed in a single integrated circuit (IC) package or a multi-IC package. A package provides additional protection against tampering. Of course, device 150 could be employed without any IC packaging if additional protection is not desired.

Herein, device 150 comprises a processing unit 200 and a persistent memory 210 (e.g., non-volatile, battery-backed random access memory "RAM", etc.). Processing unit 200 is hardware that is controlled by software that internally processes information. For example, processing unit 200 can perform hash operations, perform logical operations (e.g. multiplication, division, etc.), and/or produce a digital signature by digitally signing information using the Digital Signature Algorithm. Persistent memory 210 contains a unique asymmetric key pair 220 programmed during manufacture. Used for certifying pseudonyms, asymmetric key pair 220 includes a public key (PUKP1) 230 and a private key (PRKP1) 240. Persistent memory 210 may further include a public key 250 (PUKP2) of second platform 120, although it may be placed in volatile memory (e.g., RAM, register set, etc.) within device 150 if applicable.

In this embodiment, device 150 further comprises a number generator 260 such as a random number generator or a pseudo-random number generator. Number generator 260 is responsible for generating a bit stream that is used, at least in part, to produce one or more pseudonyms. A "pseudonym" is an alias identity in the form of an alternate key pair used to establish protected communications with another platform and to identify that its platform includes trusted device 150. The pseudonym also supports a challenge/response protocol and a binding of licensing, secrets and other access control information to the specific platform. It is contemplated, however, that number generator 260 may be employed externally from device 150. In that event, the greater security would be

realized by platform 110 if communications between number generator 260 and device 150 were protected.

Referring to Figure 3, a flowchart of an illustrative embodiment describing allocation and use of a pseudonym is shown. To fully protect the user's privacy, the user should have positive control of the production, allocation and deletion of pseudonyms. Thus, in response to explicit user consent, a new pseudonym is produced (blocks 300 and 310). Also, to access information (e.g., label, public key, etc.) that identifies an existing pseudonym, explicit user consent is needed (blocks 320 and 330). Explicit user consent may be given by supplying a pass-phrase (e.g., series of alphanumeric characters), a token, and/or a biometric characteristic to the trusted device. For example, in one embodiment, a user pass-phrase may be entered through a user input device (e.g., a keyboard, mouse, keypad, joystick, touch pad, track ball, etc.) and transferred to the trusted device. In another embodiment, memory external to the logic may contain pseudonyms encrypted with a hash value of a user pass-phrase. Any of these pseudonyms can be decrypted for use by again supplying the user pass-phrase.

Once a pseudonym has been produced and allocated for use in communications with a remote platform, this pseudonym represents the persistent platform identity for that platform/platform communications, so long as the user chooses to retain the pseudonym (blocks 340, 350 and 360).

Referring now to Figures 4 and 5, flowcharts of an illustrative embodiment of the production and certification of pseudonyms are shown. Initially, upon receiving a request by the user, the pseudonym is produced by the device in coordination with a number (block 400). A pseudonym public key (PPUKP1) is placed in a digital certificate template (block 405). The digital certificate template may be internally stored within the first platform or provided by the second platform in response to a request for certification from the first platform. Thereafter, the digital certificate template undergoes a hash operation to produce a certificate hash value (block 410).

Thereafter, the certificate hash value undergoes a transformation similar to that described in U.S. Patent Nos. 4,759,063 and 4,759,064 to create a "blinded" certificate hash value (block 415). In particular, the certificate hash value is multiplied by a pseudo-random number (e.g., a predetermined number raised to a power that is pseudo-randomly select). The pseudo-random power is maintained in confidence within the first platform (e.g., placed in persistent memory 210 of Figure 2).

A certification request, including at least the transformed (or blinded) certificate hash value, is created (block 420). The certification request is digitally signed with the private key (PRKP1) of the first platform (block 425). A device certificate, namely a digital certificate chain that includes the public key (PUKP1) of the first platform in one embodiment, is retrieved or generated to accompany the signed certificate request (block 430). In this embodiment, the device certificate features a high-level certificate including PUKP1 and a lowest level certificate including the root certificate. Of course, the device certificate may be a single digital certificate including PUKP1. Both the signed certificate request and device certificate are encrypted with the public key (PUKP2) of the second platform and then transferred to the second platform (blocks 435 and 440).

At the second platform, the signed certificate request and device certificate are recovered after being decrypted using the private key (PRKP2) of the second platform (block 445). The public key (PUKP1) of the first platform may be obtained using a public key of the certification authority responsible for signing the device certificate (block 450). If the second platform can recover the certificate request, the second platform verifies the device certificate back to the root certificate (blocks 455 and 460). If the certificate request is recovered and the device certificate is verified, the transformed (or blinded) certificate hash value is digitally signed to produce a "signed result" (block 465). Otherwise, if either the transformed (or blinded) certificate hash value cannot be determined or the device certificate cannot be verified, an error message is returned to the first platform (block 470).

Upon receipt of the signed result from the second platform, the first platform performs an inverse transformation on the signal result. For example, in this illustrative embodiment, the first platform divides the signed result by an inverse of the pseudo-random number (e.g., the predetermined number raised to an inverse of the pseudo-random power) to recover a digital signature of the certificate hash value (blocks 475 and 480). The digital signature is stored with one or more pseudonyms for use in subsequent communications with other platforms to identify that the first platform includes a trusted device.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to

which the invention pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A method comprising:

producing a pseudonym including a public pseudonym key within a platform;

placing the public pseudonym key into a certificate template;

performing a hash operation on the certificate template to produce a certificate hash value;

performing a transformation on the certificate hash value for transmission from the platform;

receiving a signed result being a digital signature for the transformed certificate hash value; and

performing an inverse transformation on the signed result to recover a digital signature of the certificate hash value.

2. The method of claim 1, wherein the producing of the pseudonym includes generating the public pseudonym key and a private pseudonym key corresponding to the public pseudonym key.

3. The method of claim 1, wherein the placing of the public pseudonym key into the certificate template includes writing the public pseudonym key into a field of the certificate template.

4. The method of claim 1, wherein the performing of the transformation comprises:

performing a logical operation on the certificate hash value using a pseudo-random number to produce a value differing from the certificate hash value.

5. The method of claim 4, wherein the pseudo-random number is a predetermined value raised to an inverse power designated by a pseudo-random value.

6. The method of claim 5, wherein the pseudo-random value is stored in secure memory.

7. The method of claim 4, wherein the performing of the inverse transformation comprises performing a logical operation on the signed result using an inverse of the pseudo-random number.

8. The method of claim 1, wherein prior to receiving the digital signature, the method comprises:

digitally signing a certification request, including the transformed certificate hash value, with a private key of a first platform to produce a signed certification request.

9. The method of claim 8, wherein prior to receiving the digital signature, the method further comprises:

obtaining a device certificate being a digital certificate chain that includes a public key of a first platform, to accompany the signed certificate request

10. The method of claim 9, wherein prior to receiving the digital signature, the method further comprises:

transferring the signed certificate request and the device certificate to a second platform.

11. The method of claim 11 further comprising:

storing the digital signature of the certificate hash value for use in subsequent communications to a remotely located platform.

12. A device comprising:

a processing unit; and

a persistent memory including a first key pair and at least one pseudonym for use in communications with a remotely located device and in identifying that a platform containing the device is secure.

13. The device of claim 12, wherein the at least one pseudonym includes a second key pair.

14. The device of claim 13, wherein the second key pair is erased after a communication session with the remotely located device has concluded.

15. The device of claim 12 further comprising:
a number generator to assist in producing the at least one pseudonym.

16. A platform comprising:
a transceiver; and
a device in communication with the transceiver, the device including a persistent memory to contain a permanent key pair, at least one pseudonym generated internally within the device and a digital signature of a hash value of a digital certificate chain that includes a public pseudonym key of the pseudonym.

17. The platform of claim 16, wherein the device further includes:
a processing unit to (i) write the public pseudonym key into a certificate template, (ii) perform a hash operation on the certificate template to produce a certificate hash value, (iii) to perform a transformation operation on the certificate hash value.

18. The platform of claim 17, wherein the processing unit of the device further produces a digital signature of at least the transformed certificate hash value using a private key of the permanent key pair.

19. The platform of claim 16, wherein the processing unit of the device further appending a device certificate with the digital signature of at least the transformed certificate hash value.

20. The platform of claim 19, wherein the device certificate is the digital certificate chain.

ABSTRACT

In one embodiment, a method for utilizing a pseudonym to protect the identity of a platform and its user is described. The method comprises producing a pseudonym that includes a public pseudonym key. The public pseudonym key is placed in a certificate template. Hash operations are performed on the certificate template to produce a certificate hash value, which is transformed from the platform. Thereafter, a signed result is returned to the platform. The signed result is a digital signature for the transformed certificate hash value. Upon performing an inverse transformation of the signed result, a digital signature of the certificate hash value is recovered. This digital signature may be used for data integrity checks for subsequent communications using the pseudonym.

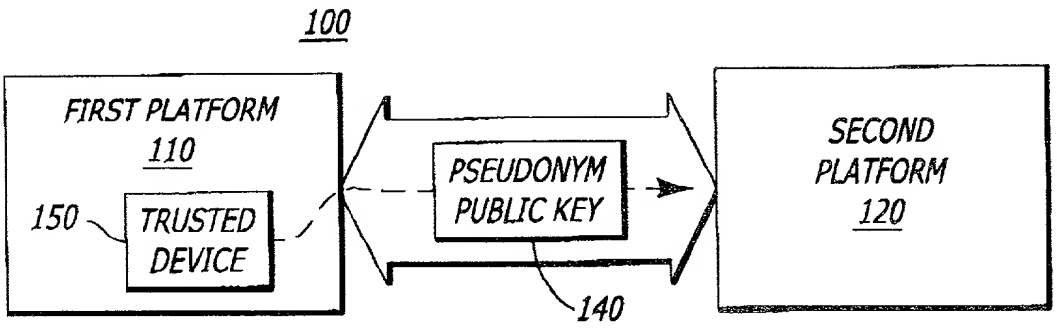

100
FIRST PLATFORM
110
150
TRUSTED DEVICE
PSEUDONYM PUBLIC KEY
140
SECOND PLATFORM
120

FIG. 1

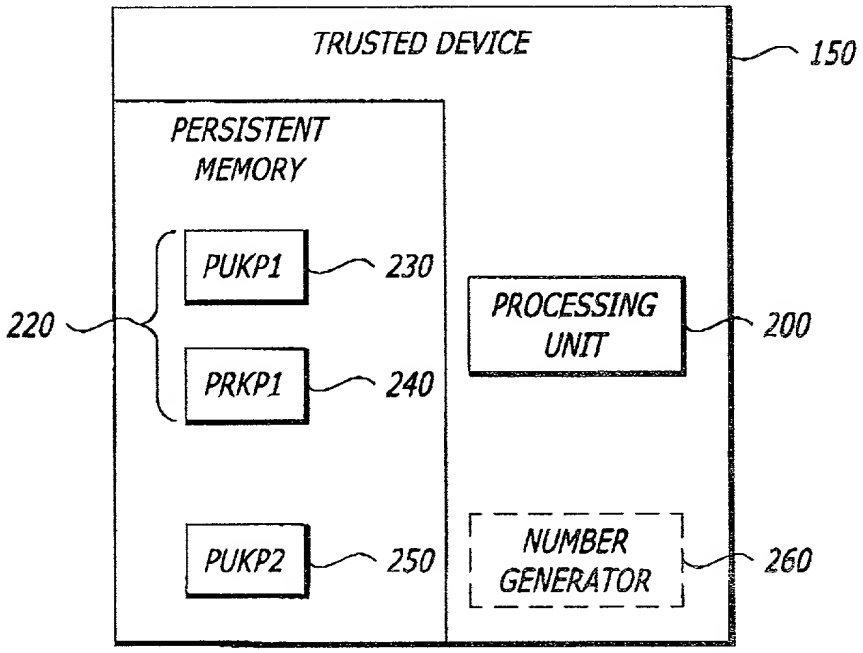
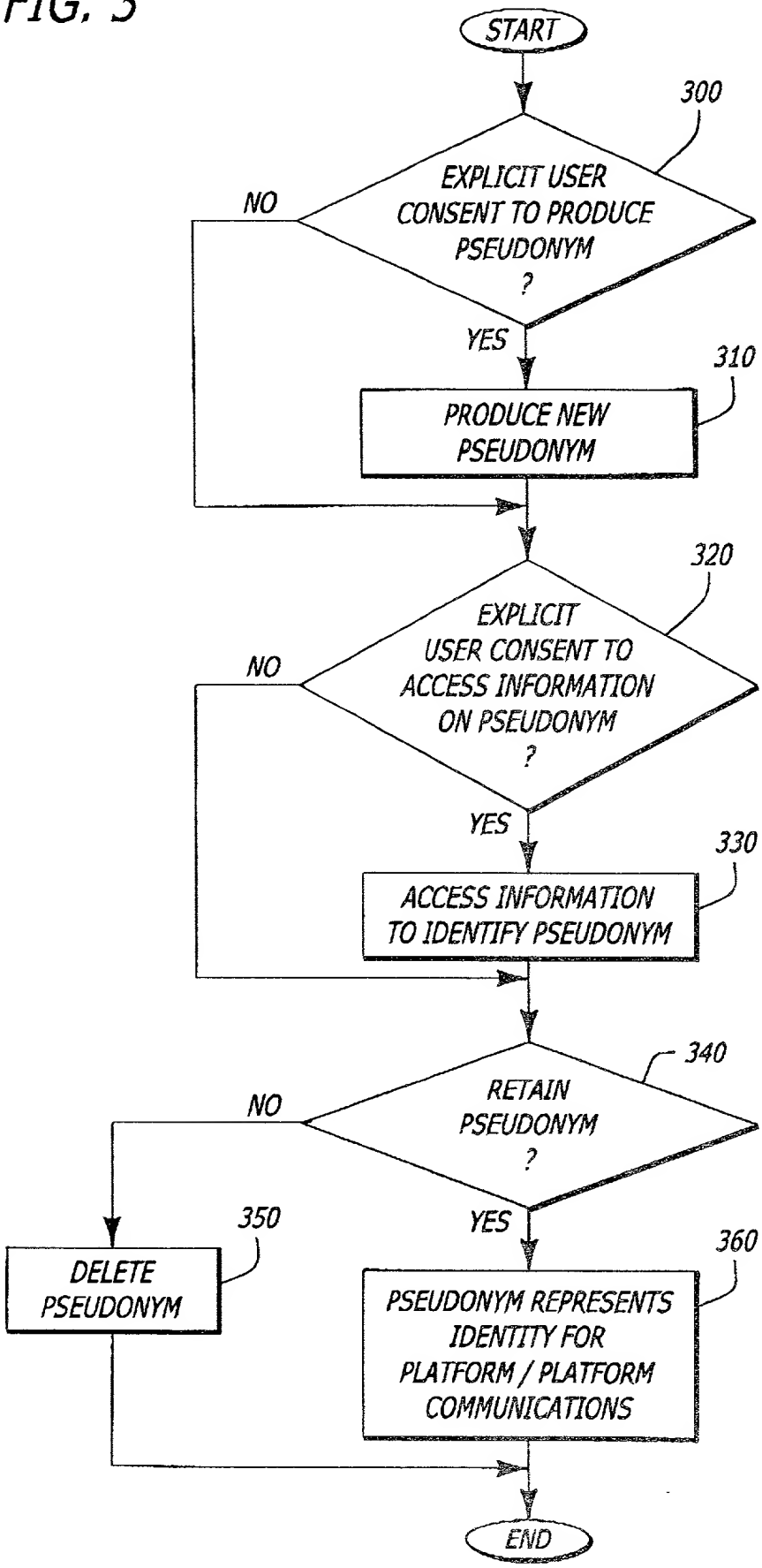

TRUSTED DEVICE
150
PERSISTENT MEMORY
PUKP1
230
220
PRKP1
240
PROCESSING UNIT
200
PUKP2
250
NUMBER GENERATOR
260

FIG. 2

FIG. 3


START
300
EXPLICIT USER CONSENT TO PRODUCE PSEUDONYM ?
NO
YES
310
PRODUCE NEW PSEUDONYM
320
EXPLICIT USER CONSENT TO ACCESS INFORMATION ON PSEUDONYM ?
NO
YES
330
ACCESS INFORMATION TO IDENTIFY PSEUDONYM
340
RETAIN PSEUDONYM ?
NO
YES
350
DELETE PSEUDONYM
360
PSEUDONYM REPRESENTS IDENTITY FOR PLATFORM / PLATFORM COMMUNICATIONS
END

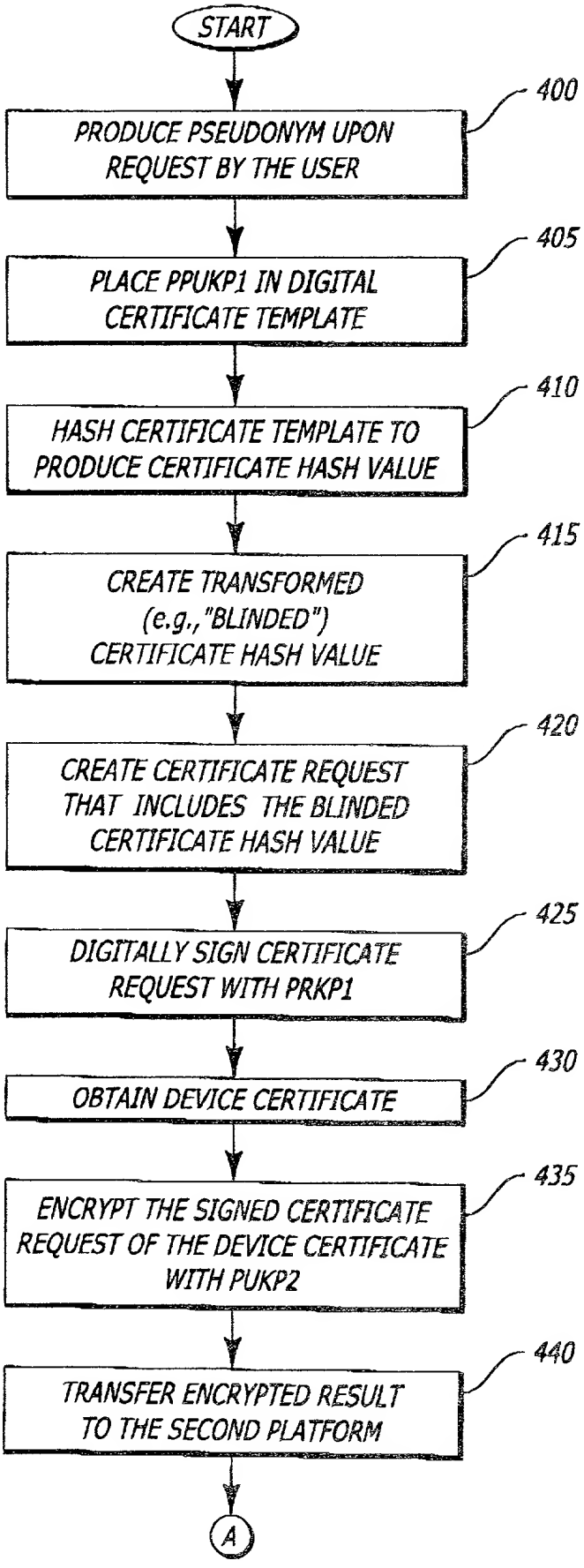

START
PRODUCE PSEUDONYM UPON REQUEST BY THE USER
400
PLACE PPUKP1 IN DIGITAL CERTIFICATE TEMPLATE
405
HASH CERTIFICATE TEMPLATE TO PRODUCE CERTIFICATE HASH VALUE
410
CREATE TRANSFORMED (e.g.,"BLINDED") CERTIFICATE HASH VALUE
415
CREATE CERTIFICATE REQUEST THAT INCLUDES THE BLINDED CERTIFICATE HASH VALUE
420
DIGITALLY SIGN CERTIFICATE REQUEST WITH PRKP1
425
OBTAIN DEVICE CERTIFICATE
430
ENCRYPT THE SIGNED CERTIFICATE REQUEST OF THE DEVICE CERTIFICATE WITH PUKP2
435
TRANSFER ENCRYPTED RESULT TO THE SECOND PLATFORM
440
A

FIG. 4

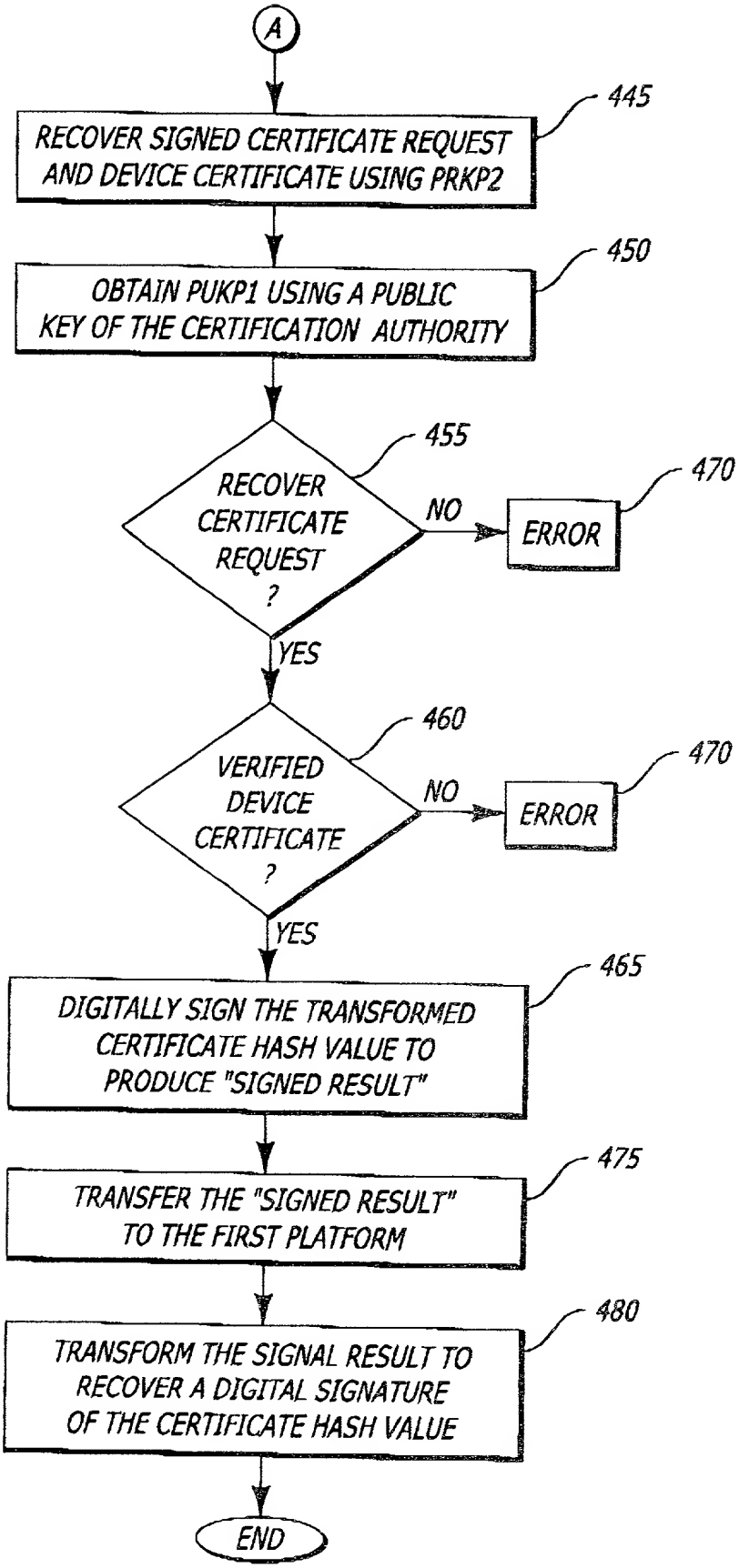

A
RECOVER SIGNED CERTIFICATE REQUEST AND DEVICE CERTIFICATE USING PRKP2
445
OBTAIN PUKP1 USING A PUBLIC KEY OF THE CERTIFICATION AUTHORITY
450
RECOVER CERTIFICATE REQUEST ?
455
NO
ERROR
470
YES
VERIFIED DEVICE CERTIFICATE ?
460
NO
ERROR
470
YES
DIGITALLY SIGN THE TRANSFORMED CERTIFICATE HASH VALUE TO PRODUCE "SIGNED RESULT"
465
TRANSFER THE "SIGNED RESULT" TO THE FIRST PLATFORM
475
TRANSFORM THE SIGNAL RESULT TO RECOVER A DIGITAL SIGNATURE OF THE CERTIFICATE HASH VALUE
480
END

FIG. 5

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY

the specification of which

[X] is attached hereto.
[ ] was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, **month**, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ No ☐ Yes
			☐ No ☐ Yes
			☐ No ☐ Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
William W. Schaal, Reg. No. 39,018, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
(Name of Attorney or Agent)
12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:
William W. Schaal, (714) 557-3800.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name) **Carl M. Ellison**

Inventor's Signature Carl M. Ellison Date 6/22/00

Residence Portland, Oregon USA (*City , State*) Citizenship USA (*Country*)

P. O. Address 1818 NW 28th Avenue

Portland, Oregon 97210 USA

Full Name of Second/Joint Inventor (given name, family name) **James A. Sutton**

Inventor's Signature _____ Date 6-22-2000

Residence Portland, Oregon USA (City, State) Citizenship USA (Country)

P. O. Address 20205 NW Paulina Drive

Portland, Oregon 97229 USA

Full Name of Third/Joint Inventor (given name, family name)

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

Full Name of Fourth/Joint Inventor (given name, family name)

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

Full Name of Fifth/Joint Inventor (given name, family name)

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

APPENDIX A

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; Amy M. Armstrong, Reg. No. 42,265; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. 44,587; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George L. Fountain, Reg. No. 36,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. 41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Darren J. Milliken, Reg. No. 42,004; Chun M. Ng, Reg. No. 36878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Lisa A. Norris, Reg. No. 44,976; Daniel E. Ovanezian, Reg. No. 41,236; William F. Ryann, Reg. No. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey S. Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; James M. Wu, Reg. No. 45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my attorneys; and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; and John F. Travis, Reg. No. 43,203; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.